
STRATEGIC HIRE
Adversarial AI Research Scientist
REQ#10744
Apply Now
OAK RIDGE National Laboratory
U.S. DEPARTMENT OF ENERGY
Office of Science

The digital world, its connections to the physical world, and the science and technology that underpin it all are the next great national security battlefield.

Join the team on the front lines.

Oak Ridge National Laboratory is making a strategic hire for an Adversarial AI Research Scientist. In this role, you will be responsible for researching, designing, and developing AI systems that can withstand attacks from malicious actors. You will work closely with a team of ORNL researchers and developers to explore different approaches to adversarial machine learning (ML), evaluate existing algorithms and methods, and develop novel techniques for improving the security and robustness of AI models.

If you are passionate about using your skills and expertise to make a difference in the world of AI, apply for this exciting opportunity. We offer a competitive salary, comprehensive benefits package, and the opportunity to work with a team of talented professionals who are dedicated to advancing the state of the art in robust AI.

This is an ORNL Strategic Hire position. Strategic hires support ORNL's primary initiative areas, strengthen Laboratory core capabilities, and develop new program directions. Strategic hires are established investigators, well qualified for leading research programs with expertise critical for responding to evolving new programs, capable of developing substantial programs, and able to take organizational leadership roles.

As a strategic hire, you will be provided internal funding to support R&D activities and needed equipment purchases as you help establish new scientific and technical capabilities at ORNL.

Translating multidisciplinary science to real-world solutions

ORNL's National Security Sciences Directorate (NSSD) delivers science and technology leadership in cybersecurity and cyber-physical resiliency, data analytics, geospatial science and technology, nuclear nonproliferation, defense manufacturing, and high-performance computing for national security missions. We draw on the Laboratory's exceptional facilities and work closely with leading researchers across the lab to translate multidisciplinary science into real-world solutions.

NSSD's **Cyber Resilience and Intelligence Division** secures our nation's most critical assets—from the energy grid and manufacturing supply chains to transportation systems and the Internet of Things devices people rely on daily. We are advancing the resilience of critical infrastructure and military systems through innovative research and development that identifies, analyzes, and defends against vulnerabilities. And through advances in identity science, machine learning, data fusion, and natural language processing, we're helping intelligence analysts identify, characterize, track, and attribute threats—both computational and human—in cyber and digital domains.

As a nation, we are becoming more reliant on artificial intelligence and machine learning technologies every day -- and for almost every aspect of our lives, including our economic and national security. AI systems are extremely powerful, but they are also vulnerable to adversarial attacks that attempt to steal, destroy, fool, influence, and tamper with such systems. AI systems can also be misused for negative purposes such as generating misinformation. New AI science and technology is needed to enhance the security, robustness, and reliability of AI systems and to identify AI-generated deepfakes and other types of misinformation. This strategic hire position is your unique opportunity to build an exciting research program with global impact.

Major Duties and Responsibilities:

- Research and develop novel techniques for defending AI systems against adversarial attacks
- Design and implement experiments to evaluate the effectiveness of different approaches to adversarial ML
- Collaborate with researchers and developers to integrate new techniques into existing AI systems
- Keep up-to-date with the latest research in adversarial ML and related fields
- Publish research papers and attend conferences to share findings and insights with the broader community

Required Qualifications:

- PhD in computer science, mathematics, statistics, or a related field
- Strong background in machine learning, with a focus on adversarial machine learning
- Experience in designing and implementing adversarial attacks and defenses
- Proficiency in programming languages such as Python and TensorFlow or PyTorch
- Ability to work independently and collaboratively in a team environment
- Strong written and verbal communication skills

Desired Qualifications:

- Proven record of technical research skills and the desire to apply these skills to the national security domain
- U.S. Q or TS Clearance
- Practical and theoretical knowledge of adversarial AI tools and methods

Our Commitment to Diversity:

As we strive to become the world's premier research institution in the sciences and technologies that underpin critical national security missions, we are committed to creating an inclusive environment that values a diverse workforce. We recognize that a breadth of perspectives, insights, and experiences are necessary to drive the level of innovation and discovery that is mission critical to national security sciences.

ORNL is an equal opportunity employer. All qualified applicants, including individuals with disabilities and protected veterans, are encouraged to apply. If you have trouble applying for a position, please email ORNLRecruiting@ornl.gov. UT-Battelle is an E-Verify employer.

Solving Big Problems

Oak Ridge National Laboratory (ORNL) delivers scientific discoveries and technical breakthroughs needed to realize solutions in energy and national security and provide economic benefit to the nation. ORNL addresses national needs through impactful research and world-leading research centers. A wide range of partnerships with other US Department of Energy (DOE) laboratories and programs, universities, and industry pairs ORNL's strengths with others for outstanding contributions to science.

Conducting R&D with Impact

ORNL researchers apply unique facilities, sophisticated tools, and signature strengths in neutron science, high-performance computing, advanced materials, biology and environmental science, nuclear science and engineering, isotopes, and national security research to benefit science and society, making it possible to

- Advance understanding, design, and use of new materials and chemical processes
- Reveal unmatched insights through computing and data
- Ensure safe, clean nuclear power and secure nuclear materials
- Produce rare isotopes for medicine, industry, security, research, and space exploration
- Increase and exploit understanding of biological and environmental systems from genes to ecosystems

6,000+
Employees, representing over 75 countries

#1
World's most intense neutron source

3,200+
Guest researchers annually

#1
World's fastest supercomputer

2,600+
Scientific publications in 2022

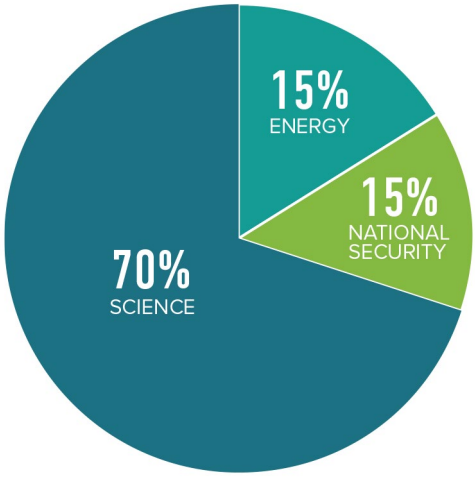
Addressing National Needs

Established in 1943 as part of the Manhattan Project, ORNL is building on a legacy of discovery and innovation to continually address the nation's most urgent R&D needs.

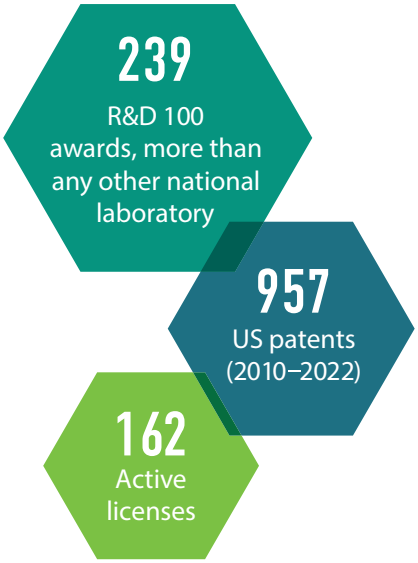
- The Proton Power Upgrade and Second Target Station will open new frontiers in materials research at the Spallation Neutron Source
- Frontier, ORNL's exascale computer, is delivering world-leading performance
- ORNL assets are focusing on national artificial intelligence and quantum initiatives
- New materials, software, and systems for advanced manufacturing developed at ORNL are transforming nuclear energy technology
- Cybersecurity technologies developed by ORNL are improving the resilience of the nation's electric grid and other critical infrastructure
- Researchers are advancing biotechnology to convert plastics into valuable chemicals

Recent R&D Highlights

- Using supercomputing and neutrons to create the most accurate 3D model of a major signaling protein in humans
- Inventing a cost-effective, environmentally friendly process to extract high-value rare earth elements from the scrapped magnets of used hard drives
- Harnessing the power of artificial intelligence to better match cancer patients with clinical trials
- Collaborating with Google to demonstrate the power of quantum computing
- Developing a process to convert ethanol into fuels suitable for aviation, shipping, and heavy-duty vehicles
- Restoring the nation's ability to produce plutonium-238 for deep space missions
- Applying human geography data and analytics for humanitarian, disaster response, and national security missions



Funding by DOE mission
FY 2022 $2.7B



Partnerships and Collaborations

- Hosting the DOE/National Nuclear Security Administration Exascale Computing Project Office
- Managing US contributions to the international ITER fusion project and leading DOE's Innovation Network for Fusion Energy
- Leading the multi-institutional Center for Bioenergy Innovation, one of four DOE Bioenergy Research Centers
- Leading two DOE Energy Frontier Research Centers
- Partnering with academia to help build a robust pipeline of scientific and technical talent
- Partnering with industry to accelerate innovation
- Collaborating with other DOE laboratories and major universities on the Cybersecurity Manufacturing Innovation Institute
- Partnering with other national laboratories, universities, and industry on the National Alliance for Water Innovation, a DOE Energy–Water Desalination Hub

Major R&D Facilities

ORNL's world-class scientific user facilities are available to users from universities, industry, and other institutions.

- Building Technologies Research and Integration Center
- Carbon Fiber Technology Facility
- Center for Nanophase Materials Sciences
- High Flux Isotope Reactor
- Manufacturing Demonstration Facility
- National Transportation Research Center
- Oak Ridge Leadership Computing Facility
- Spallation Neutron Source

Big Science. Big Impact.

Working at Oak Ridge National Laboratory

For nearly 80 years, Oak Ridge National Laboratory (ORNL) has shaped the world with discoveries in neutron science, high-performance computing, advanced materials, biology and environmental science, nuclear science and isotopes, and national security.

What ORNL Staff Say about Working Here

"At ORNL I am part of a team that is the best in what they do, and we work in an environment that encourages openness and diversity while placing a high value on research excellence and integrity. The combination of flagship strengths in quantum materials, neutron scattering, and high-performance computing coupled with the direct positive impact our work has on people's lives and the planet makes work at ORNL equal parts challenging, stimulating, and fulfilling."

—Powder Diffraction Group Leader **Clarina dela Cruz**

"Developing and applying state-of-the-art machine learning methods to complex physics applications requires exceptionally powerful and accurate computational resources in order to balance the stability, accuracy, robustness, and reliability of predictive results. With Frontier at ORNL I will be able to achieve this balance better than I could on any other supercomputer in the world."

—Computational Scientist **Max Lupo Pasini**

"When I first arrived at ORNL, I was fascinated by the lab's world-class facilities and breadth of research. As time went on I realized that nuclear processes I'd only read about were a vital part of the laboratory's fabric, and I began to meet scientists who had written the very journal articles and books I'd studied for many years. Rather than trying to glean information through reading, I simply walk across campus and meet with the world's foremost experts. The best part of working at ORNL, even as a late career scientist, is that I get to learn something new and fascinating virtually every day."

—Materials Characterization Section Head **Paula Cable-Dunlap**

$2.7B FY 2022 funding

6,000+ employees

3,200+ guest researchers annually

75+ nationalities represented in ORNL's workforce

10 highly cited researchers

2 Nobel Prizes

Contributed to the discovery of **10** elements (61, 104–106, and 113–118)

300 postdocs

957 US patents issued, 2010–2022

2,600+ FY 2022 scientific journal publications

Life at Oak Ridge National Laboratory

ORNL was established in 1943 during the Manhattan Project and, for nearly 80 years, has been a leader in science and energy research. Today, as America's largest science and energy laboratory, ORNL is a thriving multiprogram research campus with world-leading facilities and 6,000+ talented employees from over 70 countries who are innovators in their fields.

ORNL staff have innumerable opportunities to collaborate on cutting-edge scientific, operational, engineering, and support activities. In addition, ORNL offers professional development training at no cost to employees, supports numerous employee resource groups that promote diversity and inclusion efforts across the Laboratory, and provides networking opportunities.

Ideal Location

Located near the Great Smoky Mountains of Tennessee, ORNL's campus is just 1 hour away from the nation's most visited national park. Within a day's drive of all major cities on the East Coast, ORNL provides the best of both worlds: proximity to the great outdoors and growing urban centers with diverse cultural attractions. The city of Oak Ridge has 150 miles of shoreline for water recreation, rowing, and boating. Nearby Knoxville is home to the thriving research campus of the University of Tennessee and a historic downtown known for its dining, theaters, shopping, and cultural and music festivals.

In addition, East Tennessee is affordable, with a cost of living 8% lower than the national average* and no state income tax. It is one of the safest areas in the United States and has excellent school systems. The Oak Ridge Schools system is one of the highest performing school districts in Tennessee and maintains various STEM certifications.

Learn More: www.ornl.gov/who-we-are

* According to data provided by erieri.com on 1/1/2022.

Total Rewards and Amenities

Combined with competitive salaries, ORNL offers employees and their families a comprehensive and valuable benefits program. ORNL also has numerous on-site amenities that make life more convenient.

Pay & Perks

- Competitive salaries
- Bonuses and awards
- Flexible work schedule
- Professional society membership dues
- Cell phone discount
- Club ORNL discounts
- HP discount
- Apple discount
- Employee club sports

Benefits

- Medical plan (dental, vision, HSA)
- 401(k)
- Pension
- Educational assistance
- Life insurance
- Legal insurance
- Employee Assistance Program
- Generous vacation and holidays
- Wellness programs
- Disability benefits
- Pet insurance

Amenities

- Medical clinic
- Bank
- Coffee shop
- Cafeteria
- Gym
- Exercise classes
- Walking/running trails


OAK RIDGE
National Laboratory

U.S. DEPARTMENT OF
ENERGY
Office of
Science